PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 12/14, 1/00 // H04L 9/00 — A1

(11) International Publication Number: WO 98/34173

(43) International Publication Date: 6 August 1998 (06.08.98)

(21) International Application Number: PCT/DK98/00009

(22) International Filing Date: 8 January 1998 (08.01.98)

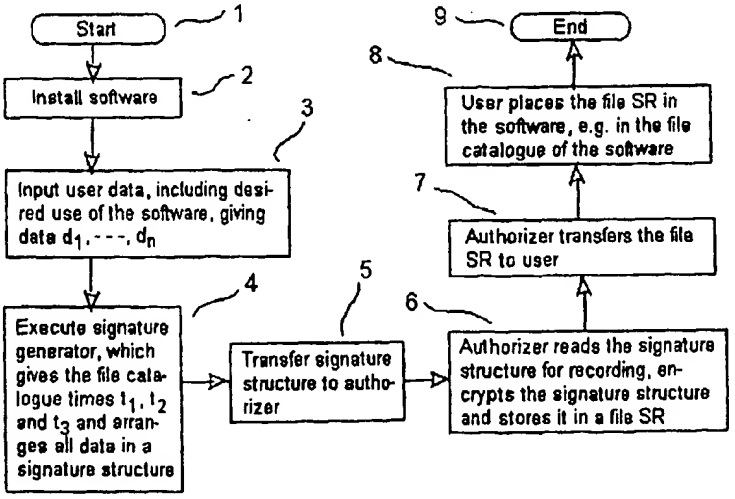
(30) Priority Data:
0029/97 9 January 1997 (09.01.97) DK

(71)(72) Applicant and Inventor: JESSEN, Hans [DK/DK]; P.O. Box 171, DK-2630 Tåstrup (DK).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
In English translation (filed in Danish).

(54) Title: A METHOD OF PREVENTING UNAUTHORIZED USE OF A COMPUTER PROGRAM



(57) Abstract

The present invention relates to a method of preventing unauthorized use of a computer program installed on a computer system. The method comprises determining a signature structure on the basis of creation times for identifiers of Cyberfiles, e.g. file catalogues. This signature structure is associated with the computer program which is able to recognize the current signature structure within certain predetermined tolerances during the execution, otherwise the execution is interrupted or changed. The invention finds use preferably for protecting computer programs and database information, including multimedia, against copying.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

A method of preventing unauthorized use of a computer program

The invention relates to a method of preventing unauthorized use of a computer program.

Existing methods are based on obtaining signatures from hardware and/or operating system(s). US Patent No. 4 688 169 discloses a method based on signatures incorporated in the operating system.

US Patent No. 4 748 561 discloses defining the signature structure from the configuration of a computer and peripheral units on the basis of the individual signatures in the hardware.

US Patent No. 5 113 518 generalizes signatures in hardware, and column 3, lines 57 - 68 exclusively mention signatures from hardware characteristics and not from e.g. file catalogues.

Generally, the existing techniques depend on hardware and/or operating system, which means that resetting of hardware/system, exchange of parts of hardware or removal of a computer program on hardware and reinstallation on new hardware, involve considerable problems in practice which significantly restrict the use of the existing techniques.

The invention uses techniques in which the signature structure is based on creation time(s) for Cyberfile(s) identifier(s). A Cyberfile is defined here as an element in the complement for ordinary files (i.e. for files placed under a file catalogue: text files, data files, executable files) on a storage medium, having an identi-

fier and an associated creation time, and, if the identifier is generated as a function of the creation time, this functional mapping must be unambiguous. A file catalogue is an example of a Cyberfile. This signature structure is unique for each individual computer system and cannot be copied by the commercially available copying programs. When programming e.g. in ANSI C: "structure" translated into 'structure' as an arranged set of components whose names in ANSI C: "identifier" translated into 'identifikator' are a user-defined data type which is to be declared so that it can observe the creation time.

The invention thus relates to a method of preventing unauthorized use of a computer program as defined in the introductory portion of claim 1, which is characterized by the features defined in the characterizing portion of claim 1.

Thus, the invention makes it possible to be independent of the hardware of the computer system by solely using the individual "historical temporal course" of the start and current operation, etc. of the computer system, which is unique to any computer system. The creation time for Cyberfiles, e.g. file catalogues, are available only with very special programming tools and not necessary for the skilled person's programming of software. Thus, the programmer as a skilled person need not consider and normally has no knowledge of how the creation times are processed according to the invention in connection with copying.

An embodiment of the method according to the invention will be described below.

A signature structure is associated with the software in which it is desired to use the invention. The signature

generator is executed in the computer system the first time the software is to be used. In this connection, the signature structure is handed over to the authorizer for reading of the authorization request, including the signature structure. The signature structure is converted by the authorizer to a form readable by a signature detector associated with the software and is subsequently stored in the software or in a file in the computer system. Subsequently, the software detects by means of a signature detector whether it can identify the stored signature structure with the detected signature structure.

The signature generator can e.g. operate in the following manner. At least one identifier is created for a file catalogue for the software to be protected against copying, followed by the determination of a desired signature structure (SR) consisting of creation times for selected file catalogues, including newly created ones. The smallest signature structure may consist of one creation time, and in that case it may be most expedient to select the creation time for the file catalogue, created in connection with the installation of the software.

The signature detector reads the stored signature structure (SR) and compares it with the signature structure (SA) of the computer system in question. If this comparison exceeds certain predetermined tolerances, the execution of the software is interrupted or changed. When comparing the authorized signature structure (SR) with the current signature structure (SA), deviations may be allowed to control the access to the entire software or specific parts of the software, including to database(s).

In order to improve the operational reliability of the copy protection technique according to the invention, the signature structure, as stated in claim 8, may contain

one or more creation times for identifiers from widely different areas of the computer system than are actually subjected to recognition. This may be expedient e.g. if some identifiers are damaged, for which reason the recognition may be performed on a selected minimum amount of the undamaged identifiers.

With a view to being able to install new versions of the computer program or e.g. extending the access to a greater part of a computer program system, including associated databases, one or more components may be added to the signature structure according to claim 9. Such components may be check/control data, e.g. version no., licence no., software code(s) for extended access. This may be useful in connection with e.g. the distribution of large computer program systems on CD ROM, where the user can e.g. merely receive a new installation disk from the supplier, which e.g. overwrites existing file(s) or writes new file(s) according to claims 4-6, and then the extended authorization may be applied for the use of the CD ROM. With reference to the latter, the invention also allows multiple installation of computer programs, as desired.

If the computer program has one or more databases attached to it, then, according to claim 9, during execution, the computer program can also compare the access code in the current signature structure with the one of the computer program, including e.g. the access code embedded in the database. This also makes it possible to prevent unauthorized use of database(s) which are attached to the computer program, also in encrypted form. This may be used to advantage e.g. on a single or specially selected user terminal(s) attached to a larger computer system.

Creation time here means the creation time in time or an unambiguous functional mapping of time in another data value, including in another data type.

Addition of one or more components in the signature structure according to claim 10, which describes future times, time intervals or accumulated execution time (real time, machine time, see the above definition of time in general), may be useful in the control of the access to the computer program or to parts of the computer program over time. It is hereby possible to incorporate a temporal functionality in the comparison. Thus, it may e.g. be ensured that the use of the computer program or part(s) thereof is prevented after 6 months. The use of time intervals e.g. allows access to the computer program for specific periods of time. When using accumulated executed time as a component, the execution of the computer program may e.g. be stopped when the use of the computer program exceeds the value of accumulated executed time determined in the signature structure.

It should be noted that, according to claim 11, component(s) of the signature structure may also be (sub)-signature structure(s) which describes/describe specific part(s) of the computer system. This may also be a useful application in computer networks.

A computer system here means any combination of hardware, operating system(s) and storage medium(media), which may also be coupled together in networks, as well as computer programs, including the installed computer program. This computer program or these computer programs are to be authorized for use by applying the principles of the invention.

The invention will now be explained more fully with reference to the embodiment shown in the drawing, in which

fig. 1 shows a block diagram of an ordinary computer system illustrated with the files incorporated in the implementation of the invention, and

fig. 2 shows a flow chart to illustrate the principles of the invention.

In fig. 1, the reference numeral 1 designates a computer system with associated storage medium 2. The software 3 is installed on the storage medium, consisting of a signature generator 4, a signature detector 5 and a stored signature structure 6.

Fig. 2 shows an example of the invention when the user is to use the software the first time. Starting from start 1 the software is installed 2. Then data 3 on the user's desired application of the software may be entered, which may be expedient in case of voluminous software with several fields of application. Then the signature generator 4 is executed, generating a predetermined amount of file catalogues in the software, reading the associated creation times and placing all data from 3 and 4 in a signature structure.

Then the signature structure is transferred 5, e.g. by facsimile, letter, file via E-mail or simple file transfer, to the authorizer. The authorizer reads 6 the signature structure to record and settle the allocated authorization, following which the signature structure is encrypted and stored in a file SR and is transferred 7, e.g. by facsimile, letter, file via E-mail or simple file transfer, to the authorizee (user).

After the user's reception of the file SR, the file SR is placed 8 in the software, e.g. the file catalogue of the software. The authorization procedure is hereby completed 9.

Patent Claims:

1. A method of preventing unauthorized use of software on a computer system, said software having already been installed on a first computer system, wherein the software, after the installation on the first computer system, has generated and, together with an authorizer, has caused storage of a signature structure for the signature of the first computer system, wherein the software, each time it is started/executed in an arbitrary computer system, checks whether the signature structure for the first computer system can be identified, and if the signature structure is not found, then the computer program represented by the software is interrupted/changed, characterized in that the software itself generates a signature structure in the form of an identification which is input in a storage in the computer system.

2. A method according to claim 1, characterized in that it is checked during the execution of the computer program whether the signature structure is within predetermined limits.

3. A method according to claim 1, characterized in that the signature structure is derived from one or more creation times for Cyberfiles in the computer system.

4. A method according to claim 1, characterized in that the storage used is located in a file in the computer system.

5. A method according to claim 1, characterized in that the storage used is embedded in the software.

6. A method according to claim 1, c h a r a c t e r - i z e d in that the storage used is compiled into the software.

7. A method according to claims 1-6, c h a r a c t e r - i z e d in that the signature structure is encrypted.

8. A method according to claims 1-7, c h a r a c t e r - i z e d in that the signature structure contains a plurality of creation times for identifiers, said plurality being larger than the plurality currently required for comparison.

9. A method according to claims 1-8, c h a r a c t e r - i z e d by adding to the signature structure component(s) which is/are check/control data providing information on version no., licence no., access code(s) to subsystem(s) of the computer program, etc.

10. A method according to claims 1-9, c h a r a c - t e r i z e d by adding to the signature structure component(s) whose value(s) determines/determine the time(s)/time interval(s)/accumulated execution time(s) for use as check/control data.

11. A method according to claims 1-10, c h a r a c - t e r i z e d by adding to the signature structure component(s) which is/are signature structure(s) for subsystem(s) of the computer system.

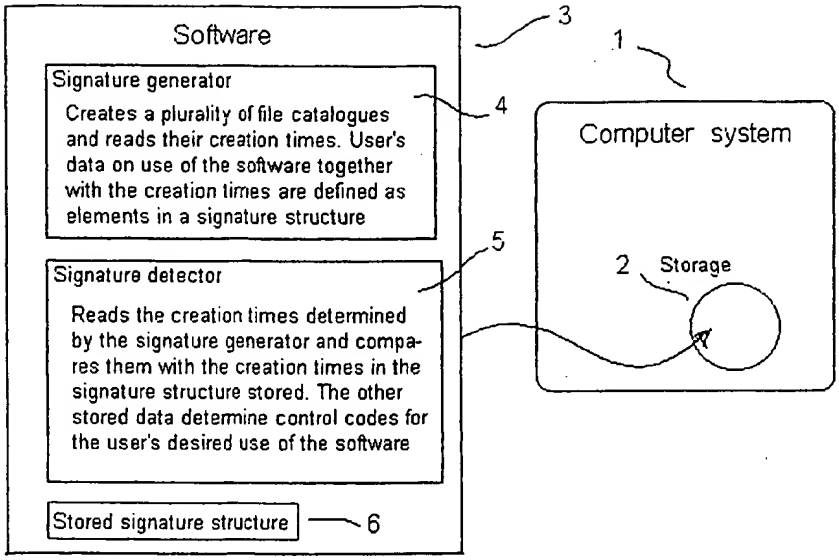

Software
Signature generator
Creates a plurality of file catalogues and reads their creation times. User's data on use of the software together with the creation times are defined as elements in a signature structure
Signature detector
Reads the creation times determined by the signature generator and compares them with the creation times in the signature structure stored. The other stored data determine control codes for the user's desired use of the software
Stored signature structure
6
3
1
4
5
Computer system
2
Storage

Fig. 1

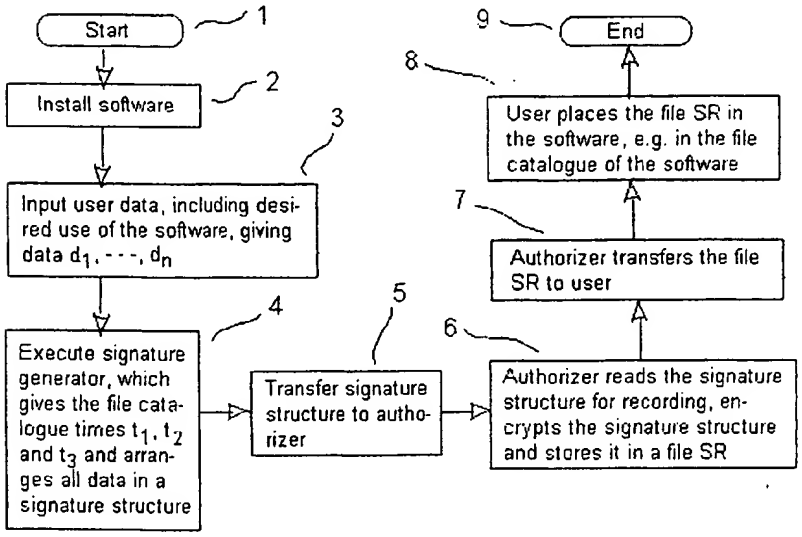

Start
1
Install software
2
Input user data, including desired use of the software, giving data $d_1, \cdots, d_n$
3
Execute signature generator, which gives the file catalogue times t_1, t_2 and t_3 and arranges all data in a signature structure
4
Transfer signature structure to authorizer
5
Authorizer reads the signature structure for recording, encrypts the signature structure and stores it in a file SR
6
Authorizer transfers the file SR to user
7
User places the file SR in the software, e.g. in the file catalogue of the software
8
End
9

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/DK 98/00009

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: G06F 12/14, G06F 1/00 // H04L 9/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPIL, DIALOG

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5113518 A (DURST JR ROBERT T), 12 May 1992 (12.05.92), page 4, figure 16B, claim 1, abstract --	1-11
X	EP 0644474 A (UNIV SINGAPORE), 22 March 1995 (22.03.95), page 3, figures 6A,7A, claim 1, abstract --	1-11
A	WO 9321582 A (LIEBERMAN MARK), 28 October 1993 (28.10.93), figure 21a, claim 1, abstract --	1-11
A	EP 0766165 A (FUJITSU LTD), 2 April 1997 (02.04.97), page 3, claim 1, abstract --	1-11

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 June 1998	02 -07- 1998
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Linus Wretblad Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/DK 98/00009

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5291598 A (GRUNDY GREGORY), 1 March 1994 (01.03.94), page 4 - page 5, claim 1, abstract -- --------	1-11

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

09/06/98

International application No.
PCT/DK 98/00009

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5113518 A	12/05/92	CA 1315001 A GB 2219421 A,B	23/03/93 06/12/89
EP 0644474 A	22/03/95	US 5412718 A	02/05/95
WO 9321582 A	28/10/93	AU 4107393 A CA 2133960 A	18/11/93 28/10/93
EP 0766165 A	02/04/97	JP 9069044 A	11/03/97
US 5291598 A	01/03/94	US 5375240 A	20/12/94

Form PCT/ISA/210 (patent family annex) (July 1992)

THIS PAGE BLANK (USPTO)